From: Bear Giles
To: Microsoft ATR
Date: 1/23/02 1:59pm
Subject: Microsoft Settlement

I am writing you to express two major concerns about the proposed Microsoft settlement.

First, Section III.J paragraphs 2(b) and 2(c) allow Microsoft to condition disclosure of API, Documentation and Communcations Protocol of the authentication system on the basis of Microsoft's determination of the viability of the requestor's business and product. As I, and many others, read these clauses Microsoft could unilaterally refuse to provide any documentation to the widely used SAMBA tools since this is an open source project with neither a business nor a viable "commercial" product.

Yet this free software - of no commercial value - is widely used to replace Microsoft Windows file and print servers with Unix servers running SAMBA. The companies benefit from reduced license fees and a perceived (and probably real) increase in reliability.

With these clauses, Microsoft could unilaterally render SAMBA sites obsolete by implementing a new authentication method for file and print sharing and refusing to disclose it to the SAMBA team on the basis of the lack of a viable commercial product. This harms the interests of the SAMBA team and of countless third-party users of their software. The sole beneficiary is Microsoft itself, since it can anticipate increased licensing fees to replace the free alternatives.

Given the conflict of interest, I would like to see the proposed settlement modified to accomodate legitimate open source projects in addition to viable commercial businesses. I understand and accept that there may need to be reasonable restrictions on what a legitimate open source project is to avoid it being used as an end-run around the commercial viability clause, but SAMBA and other major programs should certainly qualify by whatever criteria is adopted.

Second, more generally Section III.J paragraph 1(a) allows Microsoft to avoid disclosing APIs, documentation and communications protocols related to various security, encryption and rights management systems.

History has repeatedly shown that systems with documented APIs and protocols are more secure than those that keep this information secret. Public disclosure ensures that problems are detected AND FIXED as early as possible as the "white hats" quietly notify the responsible parties before public disclosure of the need to update the software.

Nondisclosure, in contrast, does little to slow down a dedicated attacker. The results are far more catastrophic since the "black hats" will not only attack anyway, they'll attack victims who have been lulled into a false sense of confidence by the "secrecy" around the API and protocols.

Ideally, I would like to see the sense of this clause reversed. Perhaps something along the lines of:

This Final Judgement shall:

1. Require Microsoft to fully document, disclose and license to third parties any and all portions of the API or Documentation or Communications Protocols related to the anti-piracy, anti-virus, software licensing, digital rights management, encryption and authentication systems, unless lawfully directed not to do so by a governmental agency of competent jurisdiction.

2. Permit Microsoft to keep confidential the specific keys and authorization tokens used with the APIs and protocols discussed above.

Respectfully,

Bear Giles
Coyote Song LLC
Boulder, Colorado
bgiles@coyotesong.com